Jaakko Ali-Keskikylä

WINDOWS SERVER 2008 R2 JÄRJESTELMÄN TIETOTURVAN HALLINTA

Tietotekniikan koulutusohjelma

2012

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

WINDOWS SERVER 2008 R2 JÄRJESTELMÄN TIETOTURVAN HALLINTA

Ali-Keskikylä, Jaakko
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Elokuu 2012
Ohjaaja: Vainio, Olli
Sivumäärä: 29

Asiasanat: Tietoturva, ylläpito, virustorjuntaohjelmat

Tämän opinnäytetyön aiheena oli Microsoft Server 2008 R2 käyttöjärjestelmän ja siihen liitettyjen asiakaskoneiden hallinta ja tietoturva. Työssä esitellään hallintaa ja tietoturvaa pienen testiverkon avulla.

Toinen keskeinen ohjelmapaketti opinnäytetyössäni on F-Securen Policy Manager ja asiakaskoneisiin asennettava F-Secure Client Security. Nämä yhdessä verkon muiden ominaisuuksien kanssa tekevät tietokoneiden käytöstä turvallista ja hallinnoinnista sujuvaa ja helppoa.

Kerron työssäni millaisia uhkia tietoturvalle on olemassa ja kuinka niiltä voidaan välttyä. Koska kuva kertoo enemmän kuin tuhat sanaa, käytän työssä paljon kuvia joissa näkyy mm. valikoita ja tapahtumia.

Kokonaisuudessaan järjestelmän käyttöönotto oli helppoa ja vaivatonta. Internet on pullollaan ohjeita ja käyttöjärjestelmäkin neuvoo jatkuvasti ominaisuuksia asennettaessa.

ADMINISTRATING SYSTEM SECURITY OF MICROSOFT SERVER 2008 R2

Ali-Keskikylä, Jaakko
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in information technology
August 2012
Supervisor: Vainio, Olli
Number of pages: 29

Keywords: Security, administration, antivirus software

The subject of this thesis was to configure and administrate Microsoft server 2008 R2 operating system and to maintain security on client computers connected to it. Network administration and security features were tested in a small network.

Another important software package used in my thesis was the "policy manager" for the server and "client security" for the client computers. Both are made by a Finnish company called F-Secure. These two programs together with other features and roles of server and network create an easy-to-use and a safe environment for users and administrators.

In this thesis I am explaining what kind of threats exists to information security and how to avoid them. Because one picture is more than a thousand words I am using a lot of screenshots to show what I am currently doing.

Overall the initialization of the system was easy and effortless. The internet is full of instructions and the system itself is advising constantly while installing new features.

SISÄLLYS

TERMIT

Server 2008	Microsoftin käyttöjärjestelmien server-tuoteperheen uusin versio, Server 2008 R2. Julkaistu helmikuussa vuonna 2008.
Windows 7	Microsoftin uusin käyttöjärjestelmä. Julkaistu loppuvuonna 2009.
Windows XP	Maailman yleisin käyttöjärjestelmä asiakaskoneissa hieman yli 40% osuudella(helmikuu 2012) /2/
Client	Asiakaskone. Tietokone joka toimii verkon alaisuudessa.
Haittaohjelma	Näitä ovat esimerkiksi virus, troijalainen, mato, vakoilu- ja mainosohjelmat.
Palomuuri	Suodattaa dataliikenteestä haitallisen tai turhan liikenteen pois hyödyllisen seasta.
NAP	Network access protection. Microsoftin server 2008 järjestelmän ominaisuus verkkoon päästettävien asiakaskoneiden verkko-oikeuksien hallintaan.
NAT	Network address translation. IP- osoitteen muunnostekniikka, jolla voidaan piilottaa tai säästää julkisia IP- osoitteita. Hyödyllinen kun käytössä on rajallinen määrä julkisia osoitteita, tai halutaan pystyttää turvallisempi lähiverkko.
DHCP	Verkko-osoitteiden jakamisprotokolla.

DNS	Nimipalvelujärjestelmä. Muuttaa numeroista koostuvat osoitteen ihmiselle helpommin muistettavaan muotoon.
BIOS	Basic Input-Output System. Ohjelma joka lataa käyttöjärjestelmän tiedostot keskusmuistiin koneen käynnistyessä.

1 JOHDANTO

Työn tarkoituksena oli perehtyä Server 2008 R2:een, Microsoftin uusimpaan palvelinkäyttöjärjestelmään, ja F-Securen keskitettyyn tietoturvan hallinta-ohjelmistoon sekä näiden kahden yhteistoimintaan.

Erilaiset virukset ja muut haittaohjelmat ovat lisääntyneet jatkuvasti. Aikaisemmin haittaohjelmien tarkoituksena oli lähinnä vain tekijöiden näyttämisen halu ja niistä aiheutui yleensä vain pientä kiusaa. Viime aikoina rikolliset ovat pyrkineet saamaan taloudellista hyötyä haittaohjelmilla ja niiden torjunnan merkitys on entisestään kasvanut.

Server 2008 R2 ilmestyi myyntiin loppuvuonna 2009 ja se sai ensimmäisen service pack päivityksen helmikuussa 2011. Työn kohteena on siis varsin tuore järjestelmä, joka sisältää uusia mielenkiintoisia tietoturvaan liittyviä piirteitä.

Alunperin ajattelin työn aiheen olevan vain tuon käyttöjärjestelmän tietoturva, mutta ohjaava opettaja huomautti F-Securen uudesta Policy Managerista, joten otin myös sen mukaan. Palvelinkoneeseen asennettiin F-Securen Policy Manager ja asiakaskoneisiin F-Secure Antivirus keskitetyllä hallinnalla.

Työ alkoi laitteiden ja käyttöjärjestelmien asennuksella. Myöhemmin kokoonpanoon lisättiin laitteita ja käyttäjiä. Lopullisessa kokoonpanossa oli neljä tietokonetta, yksi reititin ja yksi palomuuri. Käytettävissä asiakaskoneissa oli käyttöjärjestelminä Microsoft Windows XP service pack 2, Microsoft Windows XP service pack 3, sekä Microsoft Windows 7 service pack 1.

2 VERKON TIETOTURVA

2.1 Haittaohjelmat

Haittaohjelmia on monenlaisia. Toisten tarkoitus on häiritä käyttäjää ja toiset taas valjastavat koneen hyökkääjän haluamaan käyttöön. Tällaiset kaapatut koneet muodostavat ns. botnet-verkkoja, joiden yhteiskäytöllä voidaan saada suurtakin vahinkoa aikaan. Käyttäjä ei usein edes tiedä koneensa olevan myös jonkun muun käytössä. /4/

Botnet verkoilla voidaan esimerkiksi ylikuormittaa palvelimia niin että ne eivät toimi kuin osittain tai menevät jopa kokonaan ”alas”. Toinen tapa käyttää näitä saastuneita koneita on laittaa ne lähettämään roskapostia tai levittämään haittaohjelmaa eteenpäin.

Microsoft on viime aikoina onnistunut hajottamaan tällaisia botnet verkkoja ja hidastamaan niiden kasvua. Nämä vastaiskut perustuvat uhrikoneita ohjaavien ohjauspalvelinten alasajoon. /5/

Virukset ovat haittaohjelmia, jotka haittaavat tietokoneen käyttöä, tuhoavat tiedostoja tai estävät jonkin ominaisuuden käytön. Virusten ominaispiirre on että ne monistavat itseään ja leviävät nopeasti esimerkiksi sähköpostien liitetiedostojen kautta. Viruksia on ollut olemassa jo kauan, sillä vanhin tietokonevirus on luotu jo 1982, eli noin 30 vuotta sitten.

Mato on samankaltainen haittaohjelma kuin virus, mutta se ei tarvitse levitäkseen isäntäohjelmaa ja sen tihutöiden kohteena on verkkoliikenne.

Troijalainen on usein naamioitu niin, että se näyttää tekevän jotain hyödyllistä, mutta samalla tekee haittaa. Tällaisen haittaohjelman sisään voi kätkeä lähes mitä tahansa haitallista koodia kuten viruksia tai takaportin avaajia, joilla voidaan tehdä kiusaa koneen käyttäjälle. Pankkitroijalainen on haittaohjelma, joka aktivoituu käyttäjän mennessä oman nettipankkinsa

sivulle. Se pyrkii tekemään tilisiirtoja käyttäjän syöttämillä tunnuksilla ja avainluvuilla. Monet pankit ovat siirtyneet käyttämään eri avainlukuparia jokaista siirtoa varten, joten samalla lukuparilla ei voida suorittaa toimintoja taustalla.

2.2 Käyttäjäsalasanojen murtaminen

Tiukastakaan verkon tietoturvasta ei ole hyötyä, jos järjestelmän salasana on heikko ja koneelle pääsee fyysisesti käsiksi. Internet on pullollaan erilaisia salasanan murto-ohjelmia ja resetoijia. Tässä osiossa testasin kuinka helposti eräillä tällaisilla ohjelmilla pääsee kirjautumaan sisään pääkäyttäjänä.

Useimmat tällaiset ohjelmat resetoivat halutun käyttäjän salasanan, jolloin koneen tiedostoihin pääsee käsiksi. Tämä on nopein ja kätevin keino, jos oma salasana on päässyt unohtumaan. Jos haluaa käyttäjän oikeudet jäämättä kiinni, pitää salasana murtaa. Windowsissa käytetään ns. rainbow hash- menetelmää salasanan kryptaamiseen. Tietoturvan kanssa painivien harmiksi nämä salasanan kryptaustaulukot löytyvät monesta salasanojen murtamiseen tarkoitetusta ohjelmasta.

Ensimmäinen kokeilemani ohjelma on nimeltään Ophcrack. Sen käyttö oli helppoa: Latasin levynkuva-tiedoston, poltin sen cd-levylle ja käynnistin tietokoneen tältä levyltä. Kone käynnistyi linux-järjestelmän työpöydälle, jolle käynnistyi automaattisesti salasanojen murto-ohjelma. Muutaman minuutin ajon jälkeen koneen ruudulla näkyi selväkielisenä koneen pääkäyttäjän salasana. Ruudulla näkyi myös verkon pääkäyttäjän ja asiakastilin nimet, mutta näiden salasanoja ohjelma ei pystynyt selvittämään.

Ajoin ohjelman myös Server 2008 R2 koneessa, mutta siitä Ophcrack ei saanut selvitettyä salasanoja. Toinen ohjelma, jota testasin, oli nimeltään Windows Password Breaker, tästä koitin vain ilmaisversiota. Sen maksullinen enterprise versio lupaili saavansa selville myös verkon salasanat.

Nämä ohjelmat pystyy tosin estämään kunhan BIOSin salasana on riittävän vahva ja laitteen kotelo lukittu, jottei salasanaa pääse resetoimaan.

2.3 Varmuuskopiointi

Tärkeä osa ylläpitoa on pitää huolta siitä, että tarvittaessa järjestelmä voidaan palauttaa esimerkiksi levyrikon tai vaikkapa epäonnistuneen ohjelmistoasennuksen jälkeen. Server 2008R2 versiossa tulee mukana Windows Server Backup ohjelma, jolla varmuuskopioiden ottaminen onnistuu helposti. On tosin huomattava että pienin varmuuskopioitava yksikkö on kiintolevyosio. Yksittäisiä tiedostoja tai kansioita siis ei voi varmuuskopioida. Ne voidaan kyllä palauttaa tarvittaessa yksitellen. Tämä on merkittävä muutos vanhaan Windows Backup- ohjelmaan verrattuna.
Varmuuskopio voidaan luoda sisäiselle tai ulkoiselle kiintolevylle, verkkolevylle tai dvd-asemalla levyille. /7/
Hyvä keino pitää järjestelmän data tallessa on käyttää RAID1 tekniikkaa kiintolevyjen kanssa. Tämä tarkoittaa datan peilaamista useammalle levylle, jolloin levyrikon sattuessa jää vielä vähintään yksi toimiva levy.
SSD (solid state drive) levyissä on ominaisuus, jolla levyn kirjoitettavan solun rikkoutuessa se jää luku- tilaan. Eli vaikka levy on kirjoituskelvoton, se voidaan lukea ja kloonata uudelle levylle.

2.4 Server 2008 R2:n tietoturvaominaisuuksia

- Järjestelmän palomuuri estää sekä tietokoneeseen ulkopuolelta tulevat yhteydet että tietokoneesta ulospäin lähtevät ei-toivotut yhteydet. Oletuksena poikkeuksia lukuunottamatta kaikki sisääntulevat yhteydet on estetty, ulospäin taas sallittu. Poikkeuksien teko onnistuu helposti ja ne voidaan määritellä myös ryhmäkohtaisiksi.

- Päivitykset oletuksena päällä. Päivityksiä voidaan ladata myös muille Microsoftin ohjelmille.

- Windows Defender on haittaohjelmien esto-, tunnistus- ja poisto-ohjelma. Tulee automaattisesti Vistasta lähtien, saatavilla myös vanhemmalle XP järjestelmälle.

- Internet Explorerissa käytössä suojattu tila, jolla pidetään keskeiset järjestelmän komponentit eristettynä virtualisoimalla.

- UAC (käyttäjätilien valvonta, User account control) reagoi, kun jokin yrittää tehdä muutoksia järjestelmään, ja ilmoittaa aikeista ja/tai kysyy salasanaa.

- Windowsin palveluiden tiukentaminen. Järjestelmän osia on estetty tekemästä odottamattomia toimenpiteitä. Suojaa hyvin perinteisesti Windowsin heikkoa kohtaa: Kaappaamalla on hankittu etänä paikalliskäyttäjän oikeudet ja näinollen saatu käytännössä tehtyä lähes mitä tahansa kohteena olevalle koneelle.

- Oletuksena rajattu palveluiden tarpeettomimpia oikeuksia.

- Address space layout randomization. Tekniikalla estetään muistipaikan puskurin ylivuotoa ja näin estetään ajamasta haitallista koodia järjestelmässä.

- Salakirjoitusmenetelmät laajennettu tukemaan 128- ja 256-bittisiä AES-salakirjoituksia.

- NAP (Network access protection) Ominaisuus jonka avulla voidaan automaattisesti määrittää verkko-oikeuksia asiakaskoneille perustuen koneen tietoturvan tilaan.

- Salakirjoittava tiedostojärjestelmä suojaa tiedostoja kryptaamalla ne käyttäjäkohtaisesti. Kukaan muu ei pääse tiedostoihin käsiksi.

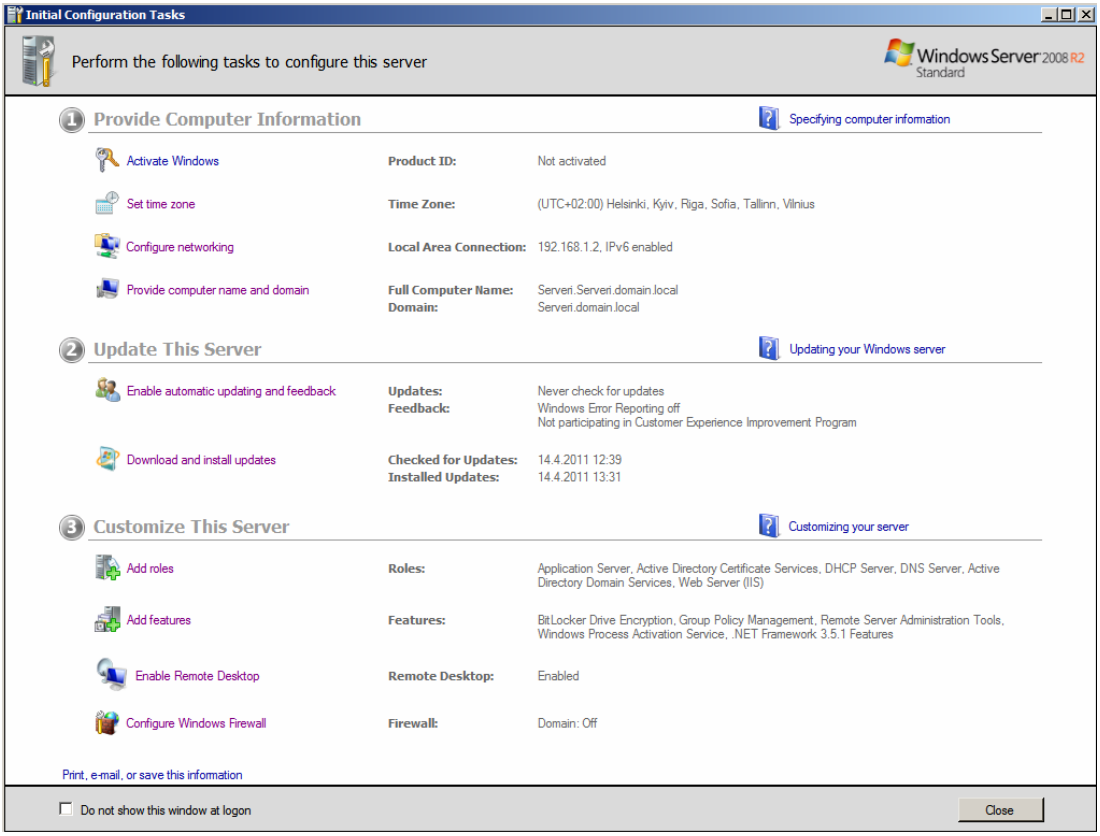
- Bitlocker. Kiintolevyn salausohjelma.

- Trusted platform modulen avulla voidaan estää koneen käynnistäminen, jos käynnistystiedostoja on muutettu. /04/

3 TESTIVERKKO

3.1 Laitteiston asennus

Ensin palomuuriin kytkettiin yksi palvelinkone, johon asennettiin käyttöjärjestelmäksi Server 2008 R2. Tähän otettiin käyttöön Active Directory (jatkossa käytetään lyhennettä AD), IP-osoitteita jakava protokolla DHCP ja nimipalvelujärjestelmä DNS. Samaan aliverkkoon kytkettiin Microsoft Windows 7 käyttöjärjestelmän päällä toimiva tietokone client- koneeksi. Tämä toimenpide oli helppo ja ongelmaton. Microsoftin uudet järjestelmät osaavat neuvoa todella hyvin käyttäjää tehtävissä asennuksissa. Esimerkiksi Server 2008 R2:en ensimmäisen kerran käynnistyessä järjestelmä avaa hallintapaneelin, jossa on tarjolla ensimmäiseksi suoritettavat toimenpiteet palvelinta konfiguroitaessa (kuva 1).



Kuva 1. Server 2008 R2:n perusasetusikkuna

Kuvassa näkyvät perusasetukset:

- aikavyöhykkeen määrittäminen
- verkkoasetukset
- tietokoneen nimi ja domain
- automaattisten päivitysten määrittely
- roolien lisääminen
- ominaisuuksien lisääminen
- etähallinnan salliminen
- palomuurin asetukset

3.1.1 AD:n käyttöönotto ja käyttäjätilien luonti

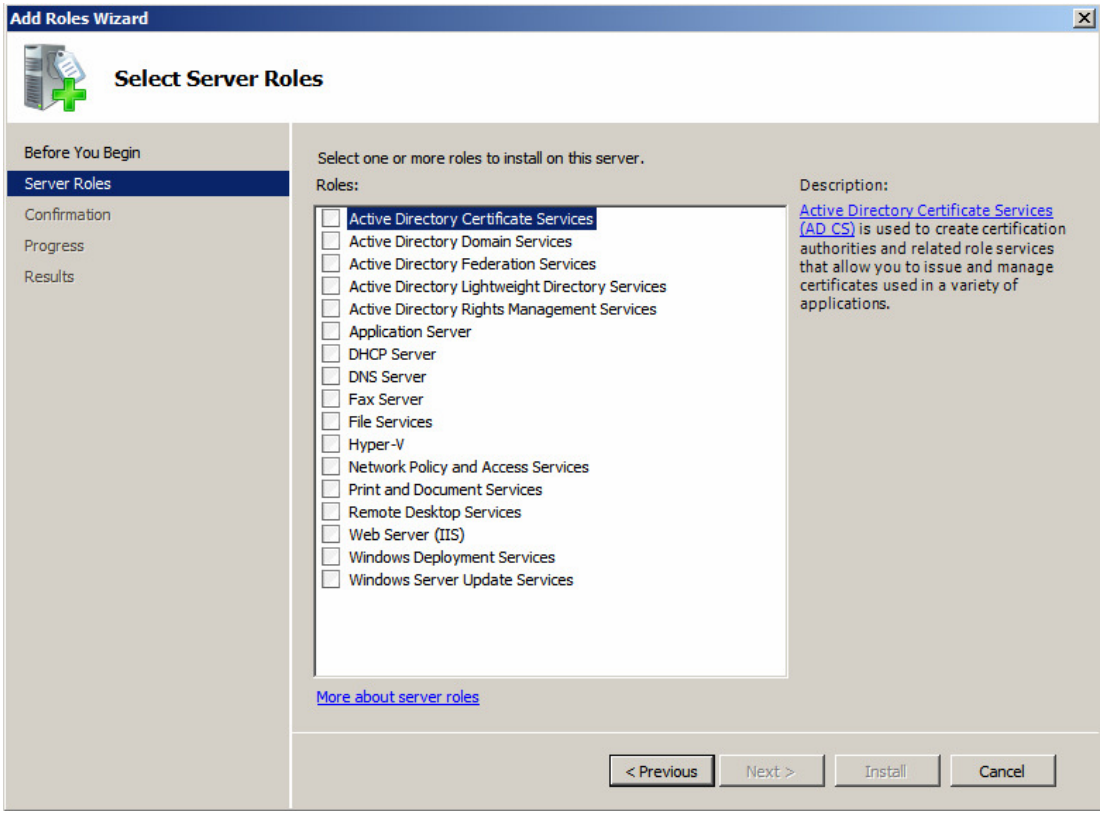
Active Directory on käyttäjätietokanta ja hakemistopalvelu. Se sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. Se mahdollistaa keskitetyn resurssien jakamisen käyttäjille ja sovelluksille sekä tarjoaa tavan hallita ja suojata käytössä olevia verkon resursseja.

/8/ http://fi.wikipedia.org/wiki/Active_Directory

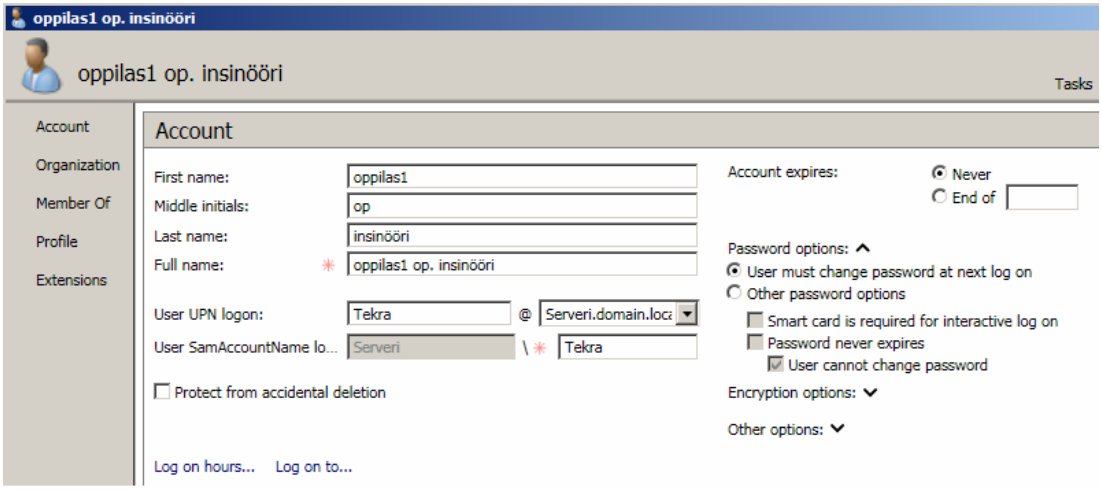
Jyrki Kivimäki, joka on kirjoittanut lukuisia kirjoja Microsoftin käyttöjärjestelmistä sekä niiden käytöstä, kertoo Active directorysta näin:

> *Active Directoryyn sisältyy hakemisto, johon kaikki verkon resursseja koskevat tiedot tallennetaan, ja palvelut, joiden avulla tietojen hyväksikäyttäminen on mahdollista. Active Directoryn tarkoitus on vähentää ylläpidettävien hakemistojen määrää, koska käyttäjien, tietokoneiden ja sovellusten hallinta voidaan tehdä yhtenäisillä rajapinnoilla ja työkaluilla. (Kivimäki, inside active directory 2003, s.6)*

AD asennetaan lisäämällä rooli serverin asetusvalikosta. Roolin lisäämispainiketta painamalla avautuu kuvan 2 mukainen ikkuna. Käyttäjätilien luonti tapahtuu Active Directoryn asentamisen jälkeen menemällä users kansioon ja painamalla new user (uusi käyttäjä). Tämän jälkeen lisätään halutut tiedot käyttäjätilistä (Kuva 3.) asettamalla kirjautumistunnukset ja oikeudet. Luodut käyttäjätilit voidaan ryhmitellä haluttuihin ryhmiin, jolloin tiettyjen oikeuksien jakaminen sujuu helposti isolle joukolle kerralla. Sama käyttäjätili voidaan asettaa useampaan kuin yhteen ryhmään, mutta oikeuksien ei tulisi olla ristiriidassa.
Asiakaskoneet liitettiin itse luotuun toimialueeseen Serveri.domain.local. Harmillisesti valitsin noinkin hankalan nimen, kun jälkeenpäin miettii. Lyhyempi ja kuvaavampi olisi ehkä soveltunut paremmin tähän työhön. Samoista tietokoneen asetuksista valittiin haluttu nimi asiakastietokoneelle, joka näkyy Active Directoryssa sekä F-Secure Policy Managerissa.



Kuva 2. Järjestelmän roolien valintaikkuna.



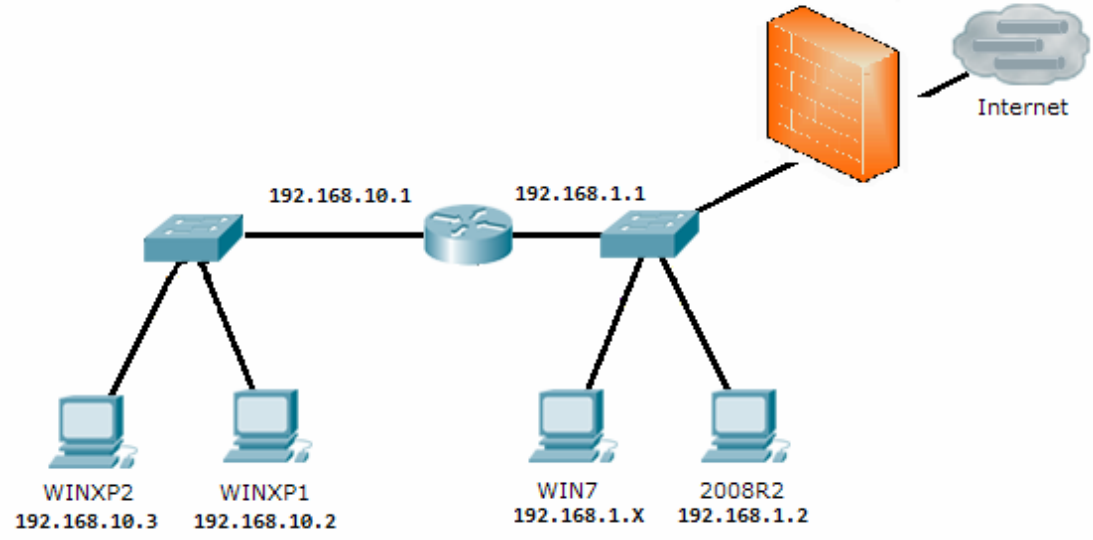
Kuva 3. Luotavan käyttäjätilin asetukset.

3.1.2 Verkon rakenne

Verkkoon lisättiin reititin ja siihen kytkettiin kaksi XP käyttöjärjestelmällä operoivaa tietokonetta. Nämä tietokoneet olivat ns. kloonatulla järjestelmällä toimivia ja tästä syystä tuli myöhemmin pieni ongelma F-Securen kanssa.

Koneet laitettiin aliverkkoon 192.168.10.0, toiselle osoitettiin IP osoitteeksi 192.168.10.2 ja toiselle 192.168.10.3.

Kokonaisuudessaan verkko koostui siis neljästä tietokoneesta, palomuurista ja reitittimestä, kuten kuvasta 4 ilmenee. Palomuuri hoiti osoitteenmuunnoksen eli NAT:n ja esti ei-toivotut yhteydet sisäverkkoon ulkoapäin.

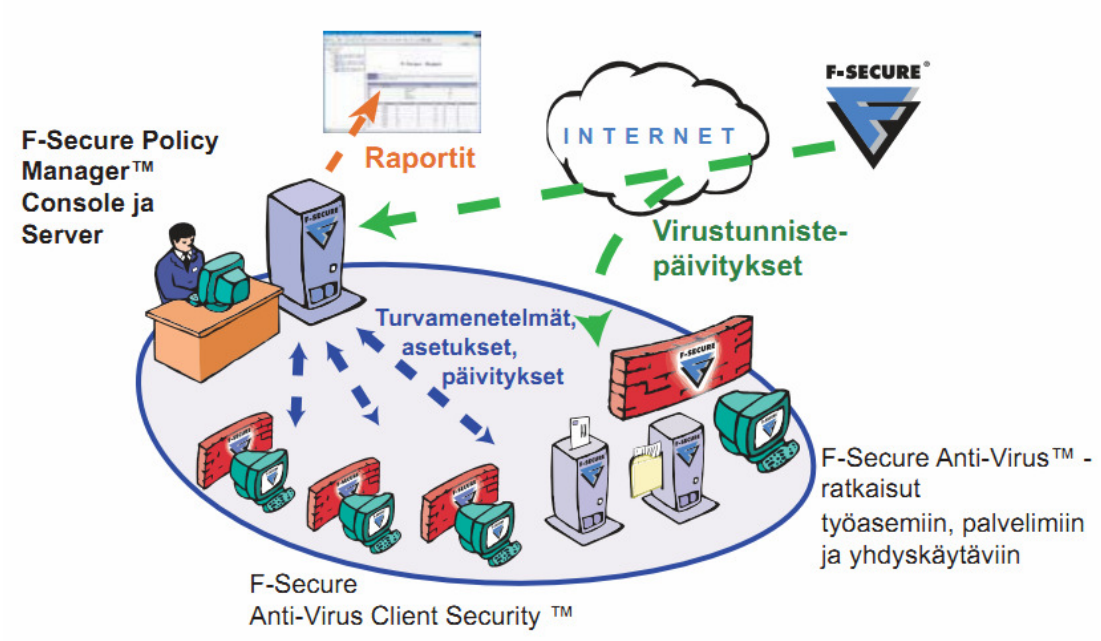


Kuva 4. Verkon rakenne.

4 F-SECURE POLICY MANAGER

4.1 Toimintaperiaate

F-Secure Policy Manager on tietoturvan keskitettyyn hallintaan tarkoitettu sovellus. Sen avulla onnistuu helposti tietoturvasovellusten asennus ja päivitys. F-Secure ilmoittaa ohjelman pystyvän hallitsemaan kerralla jopa 10 000:ta työasemaa. Melkoinen skaala ottaen huomioon, että itse käytin tuotetta laajimmillaan kolmen asiakaskoneenkoneen hallintaan. /1/ Kuvasta 5 ilmenee toimintaperiaate yksinkertaistettuna.



Kuva 5. F-Secure Policy Managerin toimintaperiaate.

4.2 F-Securen asennus

Palvelinkoneeseen asennettiin kotimainen F-Secure Policy Manager, joka on asiakaskoneiden tietoturva-asennuksia hallinnoiva ohjelma. Asennus sujui ongelmitta ja asennuskieleksi pystyi valitsemaan myös suomen. Asennettaessa ohjelma loi hiiren liikkeisiin perustuvan salausavainkooditiedoston, jota käytettiin myöhemmin asiakaskoneiden asennuksessa.

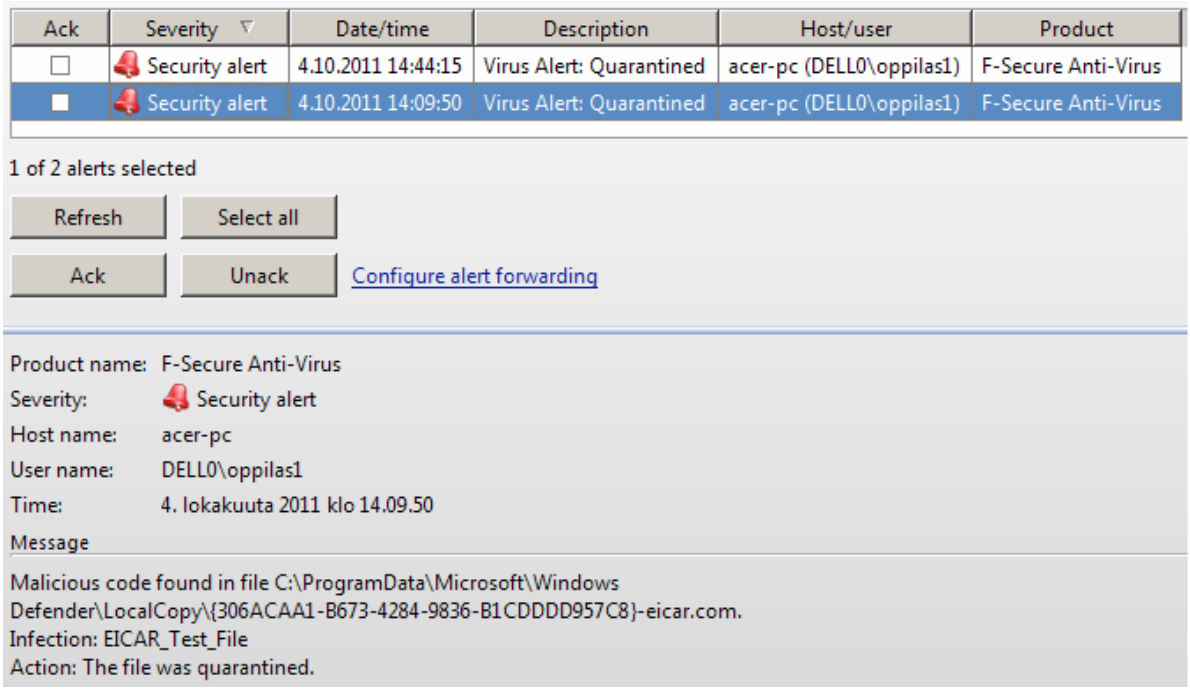
Asiakaskoneisiin asennettiin F-Secure Client Security. Asennuksen aluksi ohjelma kysyi käyttäjältä asennetaanko keskitetyllä hallinnalla käytettävä vai itsenäinen asennus. Tässä tapauksessa valitsin tietysti keskitetyn hallinnan, koska tarkoitus oli hallita asiakasversiota keskitetysti. Seuraavaksi ohjelma kysyi ”admin.pub” tiedostoa, joka on tuo aiemmin luotu salausavainkooditiedosto. Siirsin tiedoston muistitikulla kaikkiin asiakastietokoneisiin. Mikäli koneita olisi ollut enemmän, olisi ollut helpompaa ja nopeampaa luoda jaettu verkkokansio, josta asiakaskoneet olisivat voineet poimia tiedoston.

4.2.1 Ongelmia ohjelmien kanssa

Asennettuani ohjelmistot kaikkiin koneisiin huomasin, että kahdesta Windows XP koneesta vain toinen näkyi kerrallaan Policy Managerin hallintapaneelissa. Kaikki tietokoneet näkyivät kyllä oikein palvelimen käyttäjätietokannassa. Aloin ottaa selvää mistä ongelma voisi johtua ja löysinkin pian syyn oudolle käytökselle. XP koneiden F-Secure asennukset näyttivät molemmat samaa yksilöllistä tunnisteriviä: pelkkiä nollia pitkä rivi. Normaalisti tuo UID merkkisarja tulisi olla sekalaisia merkkejä eivätkä suinkaan samanlaiset.
Tutkimalla internetin keskustelupalstoja selvisi, että ongelmaa esiintyi niillä, jotka olivat asentaneet kloonatun järjestelmän päälle asennustiedostosta asiakasohjelman.
Yritin korjata ensin asentamalla puhtaan käyttöjärjestelmäasennuksen toiselle XP koneista. Tämäkään ei syystä tai toisesta auttanut, vaan kone näytti edelleen pelkkiä nollia. Onneksi koululla riitti koneita ja sain käyttööni kokonaan toisen koneen. Tähän koneeseen asentamalla käyttöjärjestelmä ja F-Secure alkoivat yhteydet toimia oikein.

4.3 Testivirusten kokeilu

Kokeilin miten Policy Manager ja asiakaskone käyttäytyvät, kun lataan “valeviruksen” internetistä. Kyseessä on siis pieni tekstitiedosto, joka ei tee mitään, mutta näyttäytyy ulkoapäin kuin olisi uhka tietoturvalle. Latasin tiedoston sekä zip-pakattuna että purettuna. Purettuun tiedostoon puuttui Windowsin oma Windows Defender. Se ilmoitti ikkunalla, että haitallinen tiedosto on löytynyt ja kysyi miten haluan toimia. Pakattuun tiedostoon se ei kiinnittänyt huomiota. Sen sijaan F-Secure löysi pakatun viruksen ja laittoi sen välittömästi karanteeniin (kuva 6).



Kuva 6. Testivirukset löytyneet asiakaskoneelta. Näkymä palvelimen ruudulta.

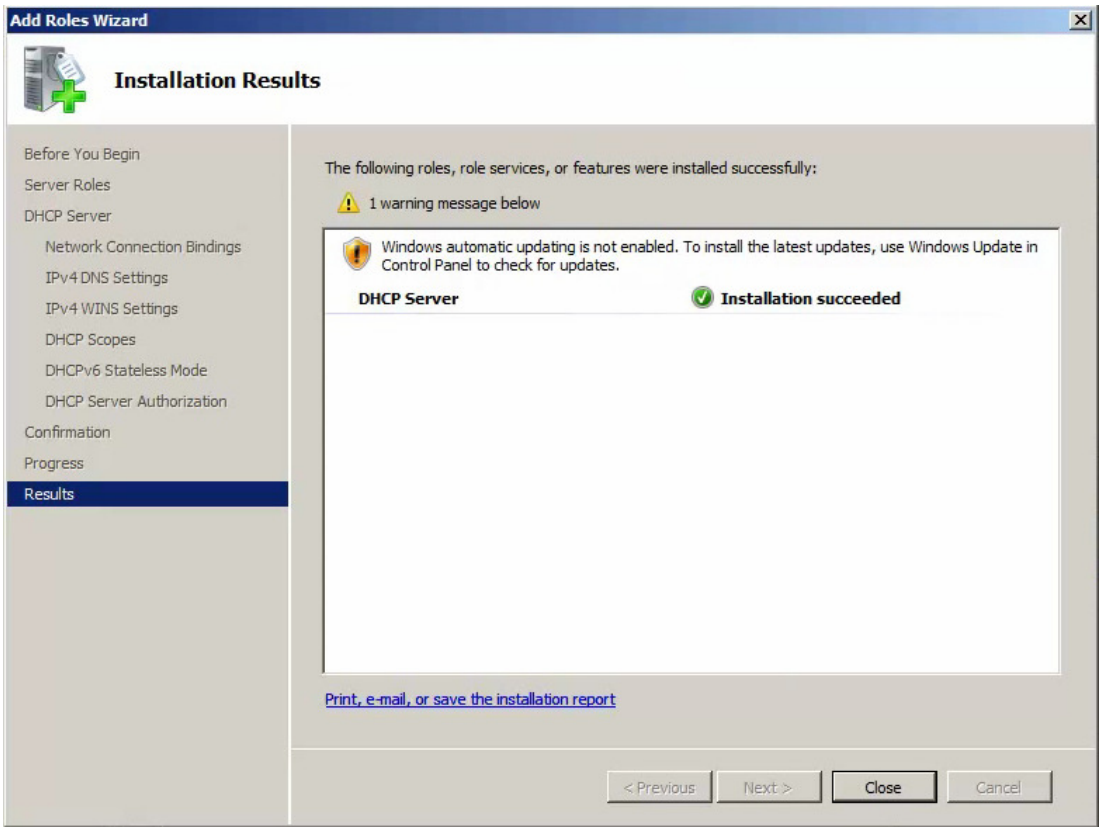
5 NETWORK ACCESS PROTECTION

5.1 Yleistä NAP:n toiminnasta

Network Access Protection (jatkossa käytetään lyhennettä NAP) on Windows server tuoteperheen uusi ominaisuus, jonka käyttö tuli mahdolliseksi 2008 versiossa. Kyseessä on ominaisuus, jolla voidaan tarvittaessa rajoittaa tai estää kokonaan jonkin asiakaskoneen verkkoon pääsy. NAP otetaan käyttöön palvelimella ja siihen voidaan luoda haluttujen määritysten mukainen rajoittava sääntö. Voidaan esimerkiksi määritellä, että koneella, jossa ei ole uusimpia järjestelmän päivityksiä, ei verkkoliikennettä sallita. Jos esimerkiksi edellämainittu sääntö ei toteudu, eli päivitykset eivät ole ajantasalla, voidaan seuraavaksi määrittää voidaanko uusimmat päivitykset hakea esimerkiksi palvelinkoneelta, vai joudutaanko käyttämään ulkoista muistia. Omat valmiit sääntöpohjat löytyvät myös esimerkiksi palomuurille, Windowsin käyttäjätilien valvonnalle(User Account Control, UAC) ja virustorjunnalle. Lisäksi voidaan tehdä verkkoliikenteen rajoituksia ja estoja kellonaikojen ja viikonpäivien mukaan.

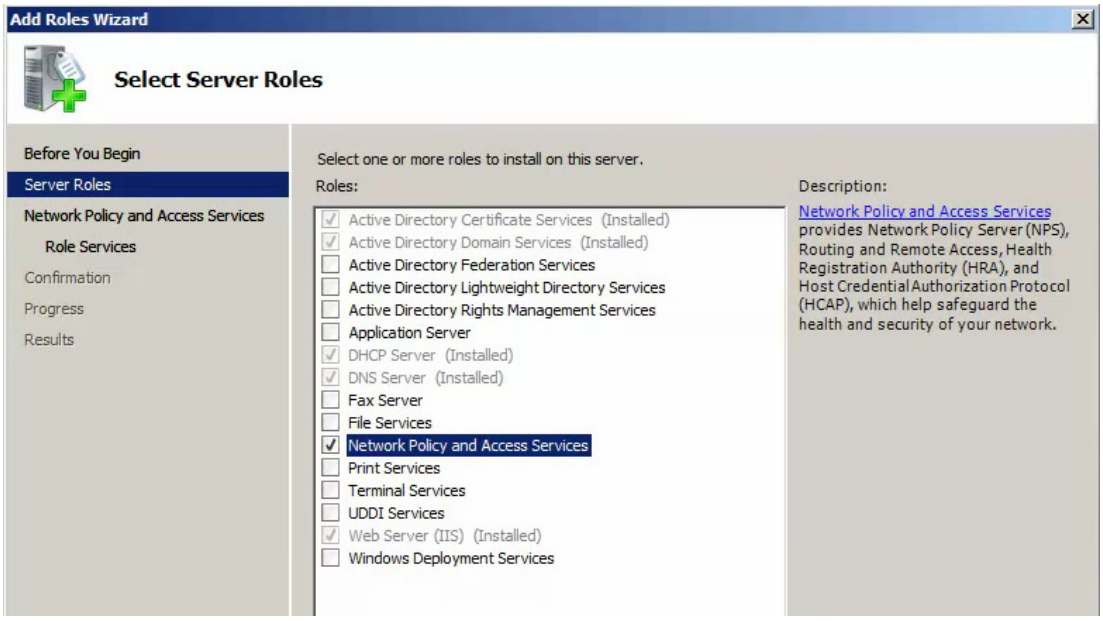
5.2 Käyttöönotto

Koska käytin työssäni vain yhtä palvelinta, asensin kaikki palvelut samalle koneelle. Ennen kuin siirrytään itse NAP:n käyttöönottoon, otetaan käyttöön DHCP server- rooli. Tämä tapahtuu kuten muidenkin roolien lisääminen. Server managerista valitaan ”Add roles”. Pakollisten tietojen syöttämisen jälkeen DHCP-roolin asennus on valmis (kuva 7).



Kuva 7. DHCP roolin asennus onnistui.

Tämän jälkeen lisätään “Network Policy and Access Services”- rooli kuten kuvassa 8.

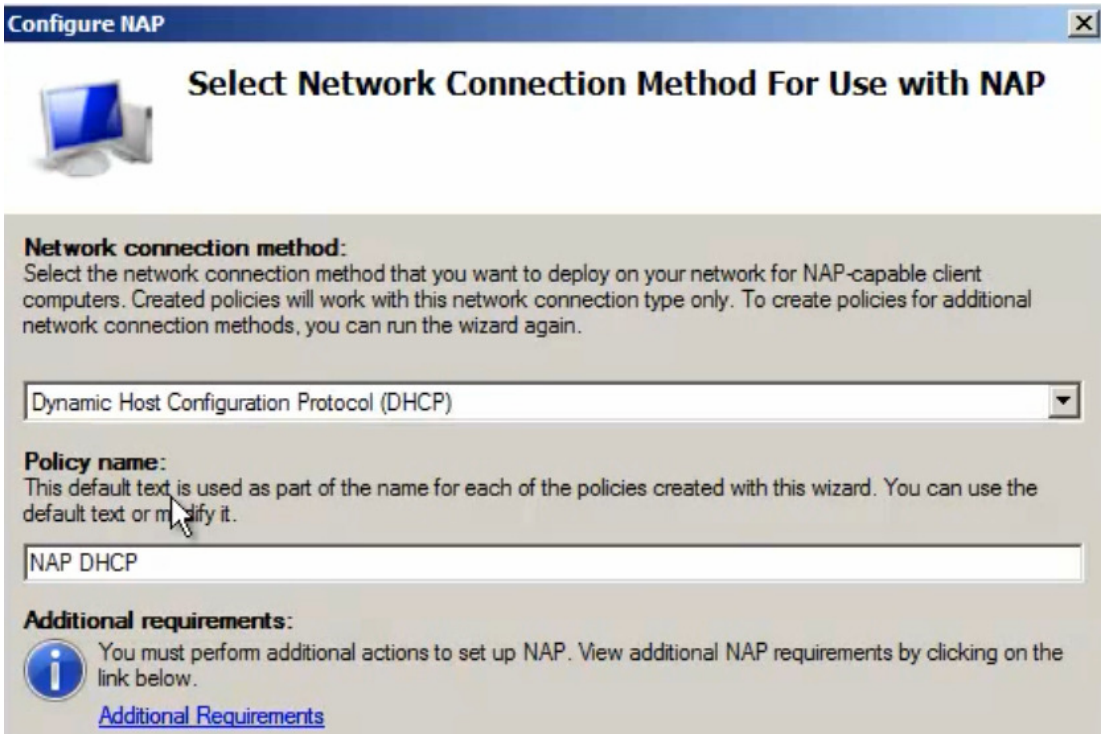


Kuva 8. Network Policy and Access Services roolin valinta.

Nyt voidaan mennä polulla käynnistä -> Administrative tools -> Network policy Server. Ensimmäiseksi pitää asettaa security health validator. Se määrittää mitkä määritteet asiakaskoneen pitää täyttää, jotta sille annetaan oikeus verkkoon. NAP -> system health validators -> windows security health -> settings. Päätin muokata default configuration tiedostoa, koska en nähnyt tarpeelliseksi luoda useampaa ohjetta.

Vaihtoehtoina on mm. onko palomuuri päällä, virustorjuntaohjelma asennettu ja automaattiset päivitykset päällä.

Seuraavaksi painetaan linkkiä Configure NAP. Asetetaan DHCP ja haluttu nimi kuten kuvassa 9.



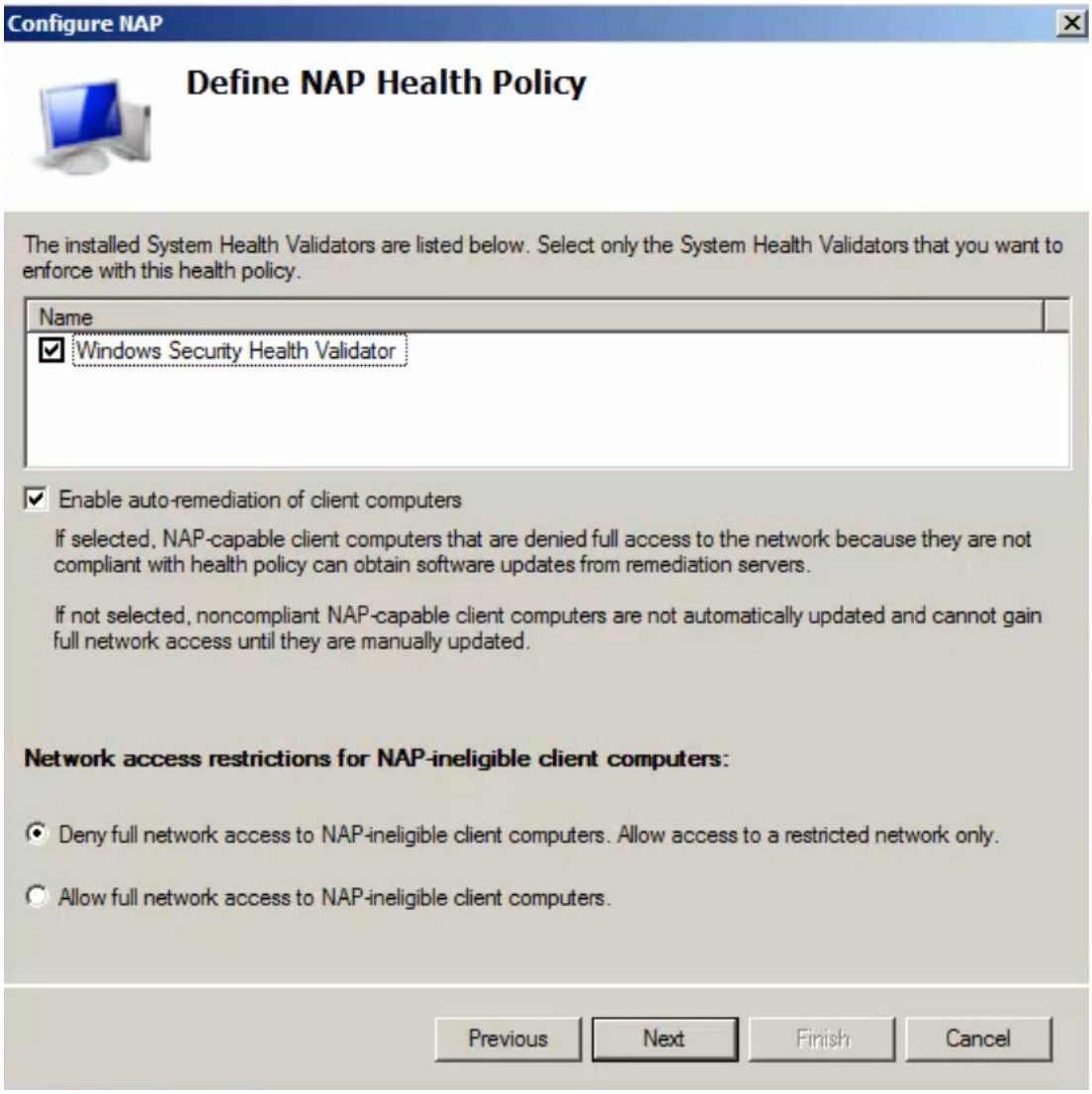
Kuva 9. DHCP:n valinta ja halutun nimen lisääminen.

Seuraavaksi kysytään RADIUS clients servereitä. Niitä ei ole käytössä, joten klikataan seuraavaan.

Valitaan haluttu DHCP-scope, eli käyttöä varten varattu osoiteavaruus. Tämän jälkeen kysytään käyttäjä- tai koneryhmiä, joihin sääntö pätee. Jos ei valita mitään, sääntö pätee kaikkiin. Jälleen kysymys RADIUksesta, joten ohitetaan.

Näiden jälkeen tulee tärkeä kysymys: Mitä tehdään koneelle jotka eivät läpäise annettuja sääntöjä. Kuten kuvassa 10 näkyy, vaihtoehtoina on antaa

oikeudet täydelle verkonkäytölle tai sallia rajatulle alueelle. Rajattu alue on tässä tapauksessa liikenne palvelimelle.



Kuva 10. Valitaan NAP säännön läpäisemättömän koneen kohtalo.

Seuraavasta ikkunasta painetaan Finish, ja NAP on asennettu.

6 BITLOCKER

6.1 Perustietoa

Bitlocker Drive Encryption on Microsoftin uusien käyttöjärjestelmien levyjen ja levyosioiden salaukseen tarkoitettu ohjelma. Ensimmäisen kerran Bitlockerin sai asennettua Windows Vista käyttöjärjestelmän laajempiin versioihin, ultimateen ja enterpriseen. Nykyjärjestelmistä myös Windows 7:n versiot ultimate ja enterprise tukevat sitä. Server 2008 pitää myös tämän ominaisuuden sisällään.

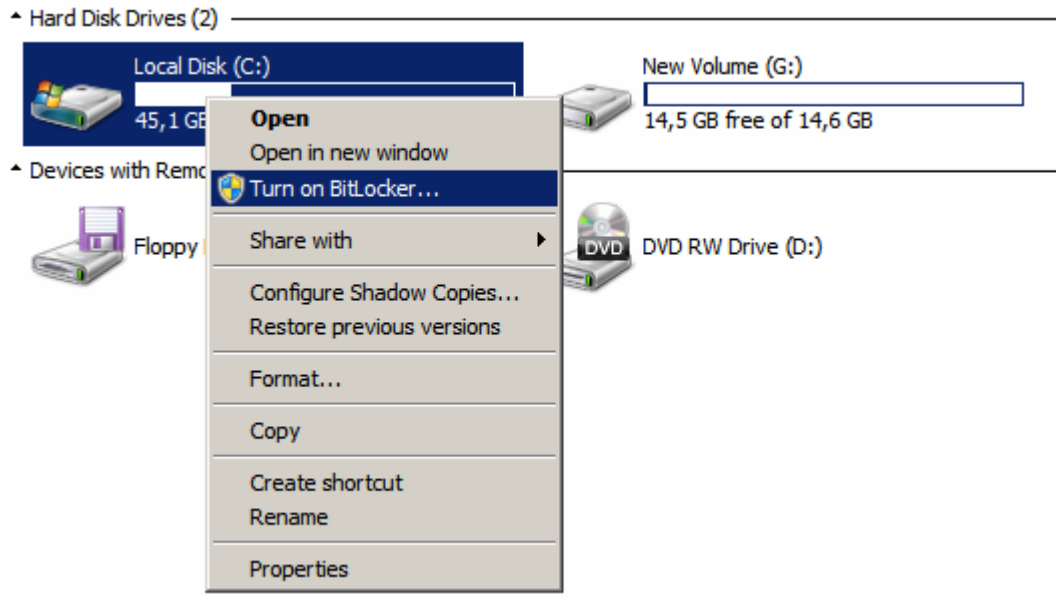
Bitlockerilla voidaan siis salata joko yksittäinen osio, kokonainen kiintolevy, tai useita levyjä. Salauksessa se käyttää AES(advanced encryption standard) salausta 128-bittisellä salausavaimella. AES on lohkosalausmenetelmä, eli se salaa tietyn mittaisen osan kerrallaan. Toistaiseksi se on murtamaton.

Bitlockerilla voidaan salata järjestelmälevy erittäin tehokkaasti. Tämä perustuu siihen, että käytetään hyväksi rautatason TPM-moduulia. TPM-piirille on tallennettu järjestelmän käynnistysdatan kuva, johon koneen varsinaista käynnistysdataa verrataan. Jos käynnistysdataa on muokattu, tietokone ei käynnisty. Muokkaamattomalla datalla tietokone käynnistyy järjestelmään normaalisti.

Bitlockerilla voidaan salata myös ulkoisia asemia. Tämä ominaisuus voidaan asettaa niin, että laite toimii normaalisti vain esimerkiksi omassa koneessa. Vaikka ulkoinen muisti varastettaisiin, se ei toimisi muissa koneissa.
/3/

6.2 Asennus

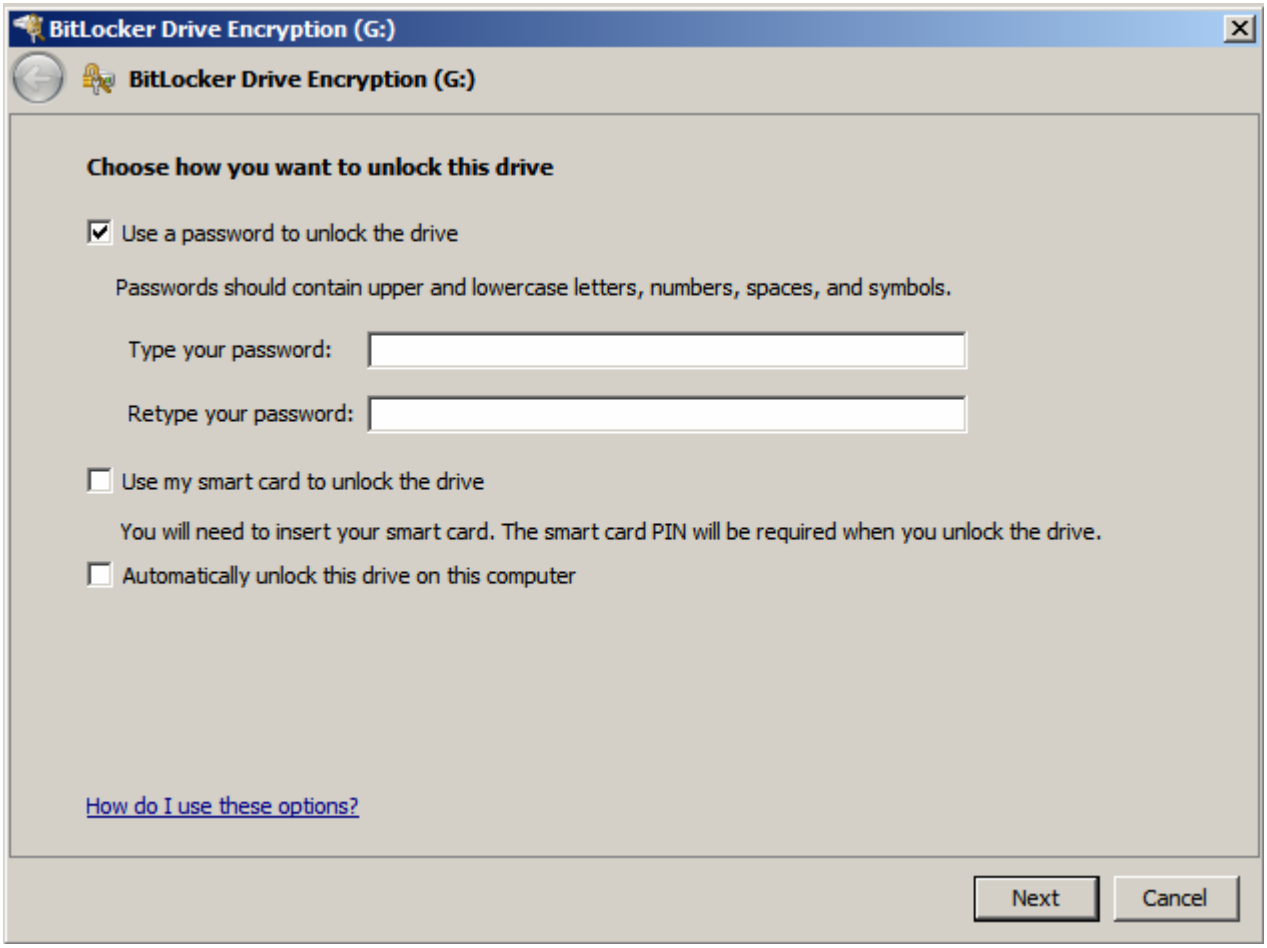
Kokeilin ensin salausta ottamatta käyttöön TPM-moduulia. Koska järjestelmälevyä ei pystynyt ohjelmalla suoraan salaamaan, lohkaisin siitä tätä kokeilua varten pienen osion. Homma alkoi klikkaamalla osion kuvaketta tietokoneesta ja valitsemalla valikosta ”turn on bitlocker”.



Kuva 11. Osion alavalikosta saa kytkettyä bitlockerin päälle.

Tämän jälkeen eteen tulevat vaihtoehdot miten varmistetaan pääsy levyllä oleville tiedostoille (kuva 12). Vaihtoehtoina on salasana, älykortin lukija tai konekohtainen salauksen avaus. Viimeisin sopii varmasti hyvin esimerkiksi ulkoiselle levylle, tai jos pelkää jonkun varastavan pelkän kiintolevyn.

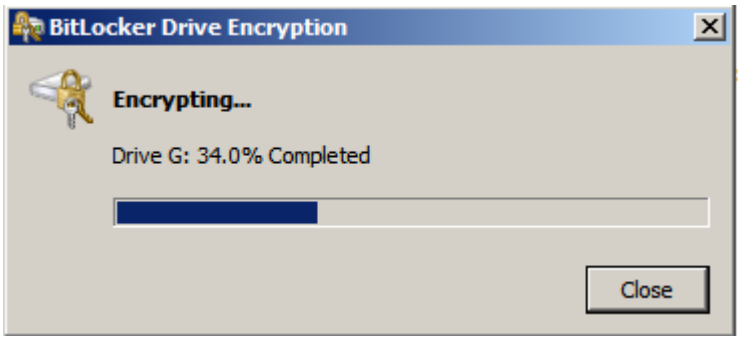
Valitsin käyttööni ylimmän, koska en omista älykortinlukijaa ja salattu osio on samalla kiintolevyllä kuin käyttöjärjestelmäkin.



Kuva 12. Haluttu tallennustapa salasanan säilytykseen.

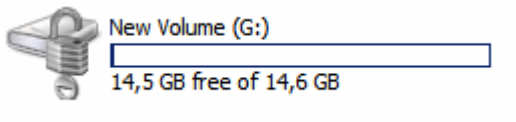
Tämän jälkeen asennusohjelma kysyy halutun säilytystavan salausavaimelle. Sen voi tallentaa joko USB-tikulle, tiedostoon koneelle tai tulostaa. Koska salausavain on tärkeässä roolissa, jos halutaan palauttaa tiedostot levyltä esimerkiksi salasanan unohtuessa, tästä kohdasta ei pääse ohi valitsematta jotain edellä mainituista vaihtoehdoista. Itse valitsin tiedostoon tallentamisen. Tässä vaiheessa tuli varoitus, ettei tiedostoa kannata pitää samalla koneella kuin salattu levy on.

Varoituksen jälkeen päästiin vauhtiin. Kuvassa 13 on jo salattu 34% halutusta osiosta. Käytössä olleella SSD(solid state drive)-levyllä 15 gigatavun osion salaus vei aikaa muutaman minuutin. Jos salattavana on esimerkiksi teratavun kiintolevy, tähän pitää varata reilusti aikaa.



Kuva 13. Osion salaaminen käynnissä.

Salaamisen jälkeen osion kuvakkeen eteen ilmestyi lukon kuva (kuva 14).



Kuva 14. Suojattu osio.

7 JOHTOPÄÄTÖKSET

Server 2008 R2 on helppokäyttöinen sekä helposti asennettava ja hallittava palvelinkäyttöjärjestelmä isoihin ja pieniin verkkoihin. Erityistä kiitosta saa järjestelmän samankaltaisuus edelliseen versioon nähden. Sen ansiosta siirtyminen uudempaan järjestelmään käy helposti. Ohjeita ominaisuuksien käyttöönottoon ja hallintaan löytyy runsaasti sekä teksti- että videomuodossa.

F-Securen antivirus- ohjelmisto asentui jokaiseen koneeseen samalla asennustiedostolla, vaikka XP:n ja 7:n ikäero on kahdeksan vuotta. Microsoft on hyvin pystynyt pitämään tuen vanhemmillekkin käyttöjärjestelmille mukana. Asennuksen jälkeen tosin ilmaantui erikoisia ongelmia liittyen palvelimelta tuleviin F-Securen ohjelmiston kättelyihin. Koneet näkyivät normaalisti F-Securen hallintaohjelmassa, mutta käskyjen jako ei toiminut vaan asiakaskone ilmoitti viasta.
Ohjelmat reagoivat välittömästi haittakoodiin, ja asettivat ne karanteeniin tai poistivat haitalliset tiedostot. Tämän perusteella uskallan suositella server 2008R2:a ja policy manageria. Molemmat olivat helppokäyttöisiä ja selvisivät halutuista tehtävistä kunnialla. Ohjelmat pitävät itsensä ajan tasalla, kunhan internet yhteys on saatavilla, ja käyttäjän huoleksi jää vain uusien käyttäjien lisääminen ja laitteiden fyysinen suojaaminen.

LÄHTEET

/1/ http://www.gnt.fi/Sivut/Esitteet/fin-pm.pdf *viitattu 1.6.2011*
/2/ http://www.netmarketshare.com/operating-system-market-share.aspx?spider=1&qprid=10 *Viitattu 15.2.2012*
/3/ http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption *Viitattu 1.3.2012*
/4/ http://www.hightechforum.fi/?j=815691 *Viitattu 13.3.2012*
/5/ http://www.tietokone.fi/uutiset/microsoft_tappoi_kertaiskulla_rikollisten_verkon *Viitattu 3.2.2012*
/6/ Windows server 2008R2 tehokas hallinta s.41,42,43, Jyrki Kivimäki 2009, kariston kirjapaino
/7/ Windows server 2008R2 tehokas hallinta s.1151,1152 , Jyrki Kivimäki 2009, kariston kirjapaino
/8/ http://fi.wikipedia.org/wiki/Active_Directory *Viitattu 10.10.2011*